NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Montana) **3 new wildfires start on Gallatin National Forest.** U.S. Forest Service officials said three new fires started in the Gallatin National Forest, located near Bozeman, Montana, the Associated Press reported July 28. The Cottonwood fire was burning west of U.S. Highway 89 along Cottonwood Creek, the Dead Deer fire in the Elk Creek Drainage, and the Mile Creek fire west of Hebgen Lake. Elsewhere, officials said the 5-square-mile Skibstad fire south of Columbus was 60 percent contained. In western Montana, the 3-square-mile Chandral Creek fire south of Darby along the Idaho border was about 60 percent contained. Source: http://missoulian.com/news/state-and-regional/wildfires/new-wildfires-start-on-gallatin-national-forest/article_22341b7c-d900-11e1-b36b-0019bb2963f4.html

National

Drought expanding rapidly, now covers 63 percent of U.S. The week of July 23, the U.S. Department of Agriculture's Drought Monitor to showed the largest 1-week jump in extreme drought growth during the report's 12-year history. Nationally, drought conditions grew for the 10th consecutive week. More than 63 percent of the contiguous United States were considered in moderate to exceptional drought. Specifically, 1,369 counties across 31 States were declared drought-disaster areas. "We've seen tremendous intensification of drought through Illinois, Iowa, Missouri, Indiana, Arkansas, Kansas and Nebraska, and into part of Wyoming and South Dakota in the last week," the author of the Drought Monitor said. The Weather Channel noted that the growth of extreme drought in the country expanded this week by 219,000 miles, an area slightly larger than the States of California and New York combined. The percentage of the continental U.S. in severe to exceptional drought set a new high for the second week straight. The drought, the most severe since the 1950s, is expected to cost at least $12 billion. Source: http://www.agprofessional.com/news/Drought-expanding-rapidly-now-covers-61-of-US---163874336.html

International

VW victim of industrial espionage in China: report. German auto giant Volkswagen (VW) has become the victim of industrial espionage in China, where its local partner has allegedly stolen engine designs, the business daily Handelsblatt reported July 27. For several months now, Chinese group FAW — with which VW has a joint venture — is believed to have copied one of the German group's engines in what sources described as "systematic and planned" espionage, the newspaper said. FAW plans to sell a model equipped with the engines in Russia, in competition with VW and Skoda models, the report continued. Source: http://www.google.com/hostednews/afp/article/ALeqM5hW-FQFU2vI96h4daVxNxMtRlMTHQ?docId=CNG.dbacd35b5162729fa3f62e1dbda6526d.2e1

Brazilian Indians hold three Amazon dam engineers hostage after talks break down. Indians were holding 3 engineers hostage at one of the work sites of the massive Belo Monte dam in Brazil's Amazon jungle following the breakdown of talks on the project's environmental impact. An official of the Norte Energia consortium building the dam said the engineers were being held against their will. According to a statement by an activist group assisting the Indians living in region, the engineers will be released after the consortium addresses the environmental concerns of indigenous groups. When completed, the $11 billion, 11,000-megawatt dam will be the world's third largest. Source: http://www.independent.co.uk/news/world/americas/brazilian-indians-hold-three-amazon-dam-engineers-hostage-after-talks-break-down-7976517.html

Russia quarantines another farming region on African swine fever. Russia's regional governor banned the transportation of hogs and the sale of pork in southern Volgograd because of African swine fever outbreaks, making it the second such area under quarantine the week of July 16, Bloomberg News reported July 20. The transportation of hogs, wild boars, and their meat was banned July 19 in the Tver region because of outbreaks of the virus, according to Russia's food safety authority. Swine fever is a viral disease that is lethal for pigs and harmless for humans, according to the United Nations' Food & Agriculture Organization. Source: http://www.bloomberg.com/news/2012-07-20/russia-quarantines-another-farming-region-on-african-swine-fever.html

Europe heat wave wilting corn adds to U.S. drought: Commodities. Heat waves in southern Europe were withering the corn crop and reducing yields in a region that accounts for 16 percent of global exports at a time when U.S. drought already drove prices to a record, Bloomberg News reported July 24. Temperatures in a band running from eastern Italy across the Black Sea region into Ukraine were approximately 5 degrees above normal, U.S. government data show. Corn, now in the pollination phase that creates kernels, risks damage, said the head of market analysis at Bourges, France-based Offre et Demande Agricole. The heat wave in Europe is adding to concern about global food supplies as U.S. farmers face the worst drought since 1956, India delays sowing because of a late monsoon, and Australian crops endure below-average rainfall. "Everyone is looking to the U.S., but clearly in Europe we'll need to import a lot of wheat and corn," said the head of market analysis at Offre et Demande Agricole, whose company advises about 5,000 farmers. Source: http://www.bloomberg.com/news/2012-07-23/europe-heat-wave-wilting-corn-adds-to-u-s-drought-commodities.html

Banking and Finance Industry

Payment terminal flaws shown at Black Hat. Three widely deployed payment terminals have vulnerabilities that could allow attackers to steal credit card data and PIN numbers, according to a pair of security researchers from penetration testing firm MWR InfoSecurity, IDG News Service reported July 26. The vulnerabilities were demonstrated at the Black Hat USA 2012 security conference. The researchers focused on three particular models of terminals, also

known as point-of-sale (POS) terminals. Two are popular in England but also used in the United States, while the third is widely deployed in America. The researchers declined to name the exact device models or the firms that manufacture them because they wanted to give vendors time to address the issues. Two devices had vulnerabilities in their payment applications that can give attackers control over various components of the devices, and can be exploited using specially crafted EMV (Chip-and-PIN) cards. The third device, which is popular in the United States, is a more sophisticated device utilizing a touchscreen, a smart card reader, a SIM card to communicate over mobile networks, support for contactless payments, an USB port, and Ethernet port, and an administration interface that can be accessed locally and remotely. The communication between terminals and a remote administration server is not encrypted, which means attackers can interfere with it using techniques like ARP or DNS spoofing to force the payment terminals to communicate with a rogue server. Source: http://www.computerworld.com/s/article/9229678/Payment_terminal_flaws_shown_at_Black_Hat

Micro attacks: The new fraud scheme. A small point-of-sale (POS) attack in Kentucky points to a larger fraud trend impacting banking institutions and their customers, BankInfoSecurity reported July 25. "Micro attacks" is the term a Gartner analyst used to describe this new scheme characterized by localized fraud incidents that are relatively small in nature, eluding detection and giving the fraudsters more time to drain accounts. In the latest example, a Winchester, Kentucky-based restaurant was named as the source of a POS attack that affected scores of credit and debit accounts and more than a dozen local banks. Other institutions in different locations report similar stories: small attacks that affect a handful of card-issuing institutions, which often fail to have fraud-detection systems sophisticated enough to connect the dots to a single point of compromise. The attacks are usually waged against a certain type of POS device or system model, which hackers hit through remote-access portals. This is easy, according to the Gartner analyst, because many businesses — especially restaurants — fail to change the default passwords installed by the original equipment manufacturer, and so fraudsters find no resistance. Source: http://www.bankinfosecurity.com/micro-attacks-new-fraud-scheme-a-4980/op-1

ATM skimmers get wafer thin. Among the latest and most difficult-to-spot skimmer innovations is a wafer-thin card reading device that can be inserted directly into the ATM's card acceptance slot, Krebs on Security reported July 24. The new devices were discussed in two recent reports from the European ATM Security Team (EAST). In both reports, EAST said one unnamed country alerted them about these new kinds of devices. They record data stored on the magnetic stripe on the back of the card as it is slid into a compromised ATM. The insert skimmers require some secondary component to record customers entering their PINs, such as a PIN pad overlay or hidden camera. Source: http://krebsonsecurity.com/2012/07/atm-skimmers-get-wafer-thin/

Japanese Finance Ministry uncovers major trojan attack. Japan's Finance Ministry uncovered evidence of a major trojan cyber-attack on its computer systems that lay undetected for almost 2 years, Techworld.com reported July 24. Ministry officials admitted that the unspecified trojan,

which was not detected by the organization's security systems, was probably free to steal confidential data from January 2010 to November 2011, after which the attack suddenly stopped. A total of 123 computers inside the Ministry were infected out of around 2,000 so far checked, which prompted the organization to change hard disks on the affected machines. The latest attack bears the hallmark of a large number that have afflicted Japanese government departments in the last year, seemingly only discovered after the damage was done. Source: http://www.computerworld.com/s/article/9229534/Japanese_Finance_Ministry_uncovers_major_Trojan_attack?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Goog

Chemical and Hazardous Materials Sector

Heat sends U.S. nuclear power production to 9-year low. Nuclear-power production in the United States is at the lowest seasonal levels in 9 years as drought and heat force reactors from Ohio to Vermont to slow output, Bloomberg News reported July 26. High temperatures and droughts have limited cooling water efficiency and availability at several nuclear power plants. Generation for the 104 plants in America July 26 fell to 94,171 megawatts, or 93 percent of capacity, the lowest level for this time of year since 2003, according to reports from the U.S. Nuclear Regulatory Commission (NRC) and data compiled by Bloomberg News. Dry conditions have worsened recently, with at least 63.9 percent of the contiguous 48 U.S. states now affected by moderate to severe drought, the U.S. Drought Monitor said. "Heat is the main issue, because if the river is getting warmer the water going into the plant is warmer and [that] makes it harder to cool," a NRC spokesman said. Source: http://www.businessweek.com/news/2012-07-26/heat-sends-u-dot-s-dot-nuclear-power-production-to-9-year-low

EPA fines violators for failure to report chemical data. The U.S. Environmental Protection Agency (EPA) issued complaints seeking civil penalties against three companies for alleged violations of the reporting and recordkeeping requirements under the Toxic Substances Control Act (TSCA), the agency reported July 23. The alleged violations involved the companies' failure to comply with EPA's TSCA section 8 Inventory Update Reporting (IUR) rules that require companies to submit accurate data about the production and use of chemical substances manufactured or imported during a calendar year. Under the TSCA, penalties can be assessed up to $37,500 per day, per violation. The reporting deadline for the 2006 IUR rule ended in March of 2007. EPA's enforcement efforts have led to 43 civil enforcement actions and about $2.3 million in civil penalties against companies that failed to report required chemical data. The reporting deadline for the 2012 submission period of the Chemical Data Reporting Rule is August 15. The most recent case was against Haldor Topsoe, Inc. of Houston for violating the 2006 IUR rule for 13 chemical substances. The June 20 complaint assessed a proposed penalty of $202,779, which the company paid July 2. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/48f1bc6ddd355fe285257a44005e28ec?OpenDocument

Commercial Facilities

(California) **24 arrested at police protests in Anaheim, Calif.** The mayor of Anaheim, California, said federal officials agreed to review two deadly police shootings and announced a meeting for July 27 after a fourth day of violent protests. Authorities said as many as 1,000 demonstrators surged through downtown July 24, smashing windows on 20 businesses and setting trash fires. Police and patrol cars were pelted with rocks and bottles. The clashes followed a city council meeting in which city leaders voted to ask the U.S attorney's office to investigate weekend officer-involved shootings that killed two men and prompted a $50 million lawsuit. Protestors turned violent after they could not get into the council chambers. Some took over an intersection, and others threw rocks and vandalized cars, and threw a Molotov cocktail that damaged a police car. A gas station was shut down after reports that some protesters were seen filling canisters with gas. Police used pepper balls and beanbag rounds. Twenty adults and four minors were arrested. About five people were hurt, including a police officer, two members of the media who were struck by rocks, and some protesters who may have been injured by police or in a fight between demonstrators. Source: http://www.usatoday.com/news/nation/story/2012-07-25/Anaheim-police-protests/56470926/1

Hacker will expose potential security flaw in four million hotel room keycard locks. A software developer and a security researcher presented a pair of vulnerabilities he discovered in hotel room locks from the manufacturer Onity, whose devices are installed on the doors of between 4 and 5 million hotel rooms around the world according to the company's figures, Forbes reported July 23. Using an open-source hardware gadget, he can insert a plug into the lock's DC port and in some cases open the lock in a matter of seconds. However, on three Onity locks installed on hotel doors he tested at well-known independent and franchise hotels in New York, the results were mixed; only one of the three opened, and even that one only worked on the second try. Even with an unreliable method, this proved real flaws in Onity's security architecture. The locks cannot be simply upgraded with new firmware to fix the problem. New circuit boards will have to be installed in every affected lock, a logistical nightmare if millions of locks prove to be vulnerable. Source: http://www.forbes.com/sites/andygreenberg/2012/07/23/hacker-will-expose-potential-security-flaw-in-more-than-four-million-hotel-room-keycard-locks/

At least 3 men arrested in separate 'Dark Knight' incidents at movie theaters. At least three men across the country who are accused of making threats during or after watching the new Batman movie have been arrested in separate incidents, the Associated Press reported July 24. Movie goers in Sierra Visa, Arizona, panicked when a man who appeared intoxicated was confronted during a showing of the movie. The Cochise County Sheriff's office said it caused "mass hysteria" and about 50 people fled the theater. The suspect was arrested on suspicion of disorderly conduct and threatening and intimidating. A Maine man was arrested when he told authorities he was on his way to shoot a former employer a day after watching "The Dark Knight Rises," Maine State police said July 23. The suspect had been stopped for speeding, and a police search of his car found an AK-47 assault weapon, four handguns, ammunition, and

news clippings about the mass shooting that left 12 people dead July 20, authorities said. In southern California, a man at a July 22 showing of the film was arrested after witnesses said he made threats and alluded to the Colorado shooting when the movie did not start. Los Angeles County sheriff's deputies were called to a cinema complex in Norwalk after movie goers said the suspect shouted: "I should go off like in Colorado." They said he then asked: "Does anybody have a gun?" A security guard saw the suspect with a backpack on his knees in the second row, but deputies who searched the bag, the theater, and its surrounding area did not find any weapon. Source: http://www.foxnews.com/us/2012/07/24/at-least-3-men-arrested-in-separate-dark-knight-incidents-at-movie-theaters/

Communications Sector

(Tennessee) **Another copper theft at a cell tower.** A third case of copper theft at a cell phone tower was reported, according to the Cookeville Police Department in Tennessee. The thieves stole copper wire from a U.S. Cellular tower site on Bunker Hill Road July 16, according to a report by an officer. The fence around the tower was cut and copper antenna wire was cut from the fence to the tower, the report said. A U.S. Cellular employee told the officer that replacing the stolen copper would cost approximately $3,500. Source: http://www.herald-citizen.com/view/full_story/19482132/article-Another-copper-theft-at-a-cell-tower?instance=latest_articles

Critical Manufacturing

NHTSA recall notice - Mazda Tribute speed control cable connector. Mazda announced July 30 the recall of 217,500 model year 2001-2006, and 2008, Tribute vehicles equipped with 3.0L V6 engines and speed control. Inadequate clearance between the engine cover and the speed control cable connector could result in a stuck throttle when the accelerator pedal is fully or almost-fully depressed. This risk exists regardless of whether or not speed control (cruise control) is used. A stuck throttle may result in very high vehicle speeds and make it difficult to stop or slow the vehicle, which could cause a crash, serious injury, or death. Mazda will notify owners, and dealers will repair the vehicles by increasing the engine cover clearance. The safety recall is expected to begin on, or before, August 6, 2012. Remedy parts are expected to be available in mid-August 2012. Until then dealers will disconnect the speed control cable as an interim remedy, if parts are not available at the time of an owner's service appointment. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V357000&summary=true&prod_id=90738&PrintVersion=YES

Ford Escape recall linked to manufacturing problem. A manufacturing problem at a company that makes fuel lines forced Ford to recall thousands of its brand-new Escape small sport utility vehicles (SUV) due to the risk of engine fires, the Associated Press reported July 22. The company said fuel lines were "mechanically scored" or damaged on the outside during manufacturing. The lines, made by a TI Group Automotive Systems plant in Indiana, can split when pushed over a connector fitting, and leaking fuel could ignite. The recall involved 11,500

Escapes in the U.S. and Canada equipped with 1.6-liter, four-cylinder engines. Source: http://www.staceypageonline.com/2012/07/22/ford-escape-recall-linked-to-manufacturing-problem/

NHTSA investigates Jeep Grand Cherokees, Dodge Ram 1500s. The National Highway Traffic Safety Administration (NHTSA) is opening 2 new investigations into more than 335,000 Chrysler vehicles — including reports that 2 new Jeep Grand Cherokee sport utility vehicles (SUV) have caught fire, Detroit News reported July 23. The agency said it opened preliminary investigations into 106,803 2012 Jeep Grand Cherokee SUVs over leaking power steering fluid hoses and 230,000 2009-10 Dodge Ram 1500 pickup trucks over reported wheel failures. The NHTSA said it received reports of two fires in Jeep Grand Cherokees since May and a third report of leaking power steering fluid causing a loss of power steering. The fires may be the result of faulty power steering hoses that is allowing steering fluid to leak onto hot surfaces in the engine compartment, NHTSA said. In one fire, an owner said he saw leaking power steering fluid in his driveway before the Jeep caught fire. Source: http://www.detroitnews.com/article/20120723/AUTO0101/207230367/1361/NHTSA-investigates-Jeep-Grand-Cherokees--Dodge-Ram-1500s

Defense/ Industry Base Sector

California man pleads guilty in Iran missile case. A California man pleaded guilty July 26 to seeking to export missile parts to Iran via the United Arab Emirates. He changed his plea to guilty in Chicago federal court. Prosecutors said an accomplice contacted him in 2009 and asked for his help buying and exporting 10 connector adapters used in an Iranian missile system. He allegedly negotiated a purchase for $9,500 from an Illinois company that was part of a sting. The naturalized U.S. citizen from Iran will be sentenced October 30. He faces up to 20 years in prison for one count of attempting to export defense articles without a license or approval. Source: http://abcnews.go.com/US/wireStory/california-man-pleads-guilty-iran-missile-case-16863628#.UBLCYaCqHU0

(Maine) **Civilian worker charged with setting both fires aboard, near submarine in Maine shipyard.** Navy investigators said a civilian employee working as a painter and sandblaster aboard the USS Miami submarine at the Portsmouth Naval Shipyard in Kittery, Maine, was charged with setting a fire that heavily damaged the vessel in May and a second near it in June. In a complaint filed July 23 in federal court in Maine, the Naval Criminal Investigative Service said the man was charged with two counts of arson involving the submarine. The submarine has been in dry dock for an overhaul at the shipyard. Court documents indicate the man was assigned to do paint stripping in the torpedo room. He first denied involvement in the fires, then later admitted involvement. He was scheduled for a court appearance July 23. Estimates put the damage to the submarine at $400 million. Source: http://www.washingtonpost.com/national/civilian-worker-charged-with-setting-both-fires-aboard-near-submarine-in-maine-shipyard/2012/07/23/gJQAfBgO4W_story.html

Emergency Services

(Maine) **Locating emergency radio jammer in York County 'not easy'.** The Federal Communications Commission (FCC) will have trouble finding the person responsible for recent emergency radio jamming in York County, Maine, without monitoring constantly, an agency spokesman said July 24. Local authorities believed a rogue radio jammer plagued the town of Lebanon and a few other surrounding communities off and on since 2004. The perpetrator fell silent earlier this year, but the jammer resurfaced July 22, following initial reports of a multi-vehicle crash with numerous injuries. Rescue workers and police who scrambled to the scene to assess the accident found their scanners' radio signal blocked. When officials realized the signal was being interfered with, a dispatcher sent a message over the airwaves that the FCC was monitoring. The jamming stopped immediately. Source: http://www.pressherald.com/news/locating-radio-jammer-not-easy_2012-07-25.html

(California) **Four East Bay police stations investigate powdery substance found in mailed envelopes.** Four San Francisco East Bay police departments received a scare July 20 when envelopes filled with white powder showed up in their mail, sparking investigations from hazardous materials crews and the FBI. The substance in three of the envelopes, which were delivered to police in Hayward, San Leandro, and Berkeley, was not hazardous, officials said. A fourth envelope delivered to the Union City Police Department was given over to the U.S. Postal Service and the FBI for more investigation, the police commander said. The substance delivered to San Leandro was baking flour, a lieutenant said, but authorities did not identify the substance found at the other stations. No injuries were reported in any of the incidents, and the people who handled the envelopes have not shown any signs of illness, authorities said. Source: http://www.mercurynews.com/breaking-news/ci_21120351/hayward-police-station-lobby-shut-down-after-powdery

Energy

(Michigan) **Michigan governor declares emergency over fuel shortage.** The Michigan governor declared an energy emergency in the State July 24 due to temporary shortages of gasoline and diesel fuel in parts of the Upper Peninsula caused by the shutdown of a pipeline in Wisconsin. The emergency declaration suspends State and federal regulations that limit hours of service for motor carriers and drivers transporting gasoline, diesel fuel, and jet fuel to address the shortages, the governor said in a statement. The West Shore pipeline that carries 70,000 barrels-per-day of refined products from Chicago to Green Bay in northern Wisconsin was shut for several days after a gasoline leak was found July 17. The pipeline was restarted July 21. The pipeline, which is operated by Buckeye Partners LP, carries gasoline, diesel fuel, and jet fuel. The closed section of the line started about 10 miles northwest of Milwaukee. The leak spilled about 1,000 barrels of unleaded gasoline, according to a report the company filed with the National Response Center. Source: http://wkzo.com/news/articles/2012/jul/25/michigan-governor-declares-emergency-over-fuel-shortage/

Significant number of power plants did not obtain new source review permits, GAO says. A significant number of coal-fired electricity generating units have not obtained new source review permits as required, the Government Accountability Office (GAO) reported July 23. The Environmental Protection Agency (EPA) investigated 831 coal-fired units since 1999 through its power plant enforcement initiative, and the agency has alleged noncompliance at 467 units through notices of violation, court complaints, or settlements, GAO said. Under the Clean Air Act's new source review permitting program, new and modified industrial sources must obtain permits that require emissions limits and the installation of emissions control equipment. GAO said new source review data are not complete because EPA has not yet investigated all coal-fired units, and EPA's determinations of compliance have changed over time. The report underlined the complexity of ensuring compliance with the new source review program, which EPA, States, and local agencies do on a case-by-case basis. Source: http://www.bna.com/significant-number-power-n12884910797/

Report says offshore industry falls short on key safety monitoring. After the lethal explosion at BP's Texas City refinery that killed 15 workers in 2005, the oil industry boosted safety at industrial operations on land but never made the same improvements offshore, according to federal investigators meeting in Houston the week of July 23. The Chemical Safety Board (CSB) is set to conclude that the offshore drilling sector's focus on monitoring individual worker injuries — while ignoring bigger warning signs of "process safety" problems that could lead to emergencies — set the stage for the Deepwater Horizon disaster. The independent federal agency is reviewing the industry's long-term response to the Texas City refinery explosion in a hearing July 23. July 24, the board is set to release preliminary findings of its investigation into the 2010 Deepwater Horizon disaster that killed 11 workers and launched the nation's worst oil spill. The CSB, which has probed more than 50 industrial accidents, does not issue citations. It makes safety recommendations to plants, labor groups, and regulators. Source: http://fuelfix.com/blog/2012/07/23/chemical-safety-board-offshore-industry-falls-short-on-key-safety-monitoring/

Food and Agriculture

CDC releases annual foodborne illness data for 2011. The number of Americans falling ill from foodborne pathogens remained steady or marginally worsened in the latter half of the 2000s, and 2011 turned out to show little difference, according to the U.S. Centers for Disease Control and Prevention (CDC), which released its annual report of foodborne illness data for 2011, July 27. While the data showed a 5-year decline of E. coli O157:H7 and Shigella infections since 2007, infection rates stagnated or slightly grew for a number of other notable bacteria, including Salmonella, Campylobacter, and Listeria. According to the data, Salmonella, Campylobacter, and Listeria continue to infect numbers well beyond goals set by the U.S. government for 2010. Source: http://www.foodsafetynews.com/2012/07/cdc-release-annual-foodborne-illness-data-for-2011/

Multistate Salmonella outbreak linked to raw tuna grows to 425. Salmonella from a recalled raw tuna product served in sushi and known as Nakaochi scrape has now sickened at least 425

individuals in 28 states and the District of Columbia. Of those ill, 55 have been hospitalized, Food Safety News reported July 26. In its final outbreak update, the U.S. Centers for Disease Control and Prevention (CDC) stated the outbreak appears to be over, though additional cases may surface in the next several months if unaware food establishments continue serving the product, which is sold frozen and has a long shelf-life. The victims of the tuna scrape outbreak were infected with one of two Salmonella strains. In total, 410 fell ill with Salmonella Bareilly, while Salmonella Nchanga sickened 15. The recalled Nakaochi scrape was produced by Moon Marine USA Corporation. Retailers carrying the product are asked not to serve it. Source: http://www.foodsafetynews.com/2012/07/multistate-salmonella-outbreak-linked-to-raw-tuna-grows-to-425/

Another 76 counties declared disasters. July 25, the U.S. Agriculture Secretary designated 76 additional counties in 6 States as primary natural disaster areas due to damage and losses caused by drought and excessive heat. During the 2012 crop year, the U.S. Department of Agriculture (USDA) has designated 1,369 counties across 31 States as disaster areas — 1,234 due to drought — making all qualified farm operators in the areas eligible for low-interest emergency loans. The additional counties designated July 25 are in the States of Indiana, Illinois, Kansas, Michigan, Nebraska, and Wisconsin. The U.S. Drought Monitor reported two-thirds of the continental United States is in a moderate to exceptional drought. During the week of July 16, the portion of the U.S. corn crop rated in very poor to poor condition climbed to 45 percent, according to USDA's National Agricultural Statistics Service. Source: http://www.agprofessional.com/news/Another-76-counties-declared-disasters-163732856.html

(Alabama) **Copper thieves hitting Alabama farms.** Copper thefts are becoming a growing problem for Alabama farmers, the Associated Press reported July 25. A southeast Alabama farmer said someone stole the copper wiring from his irrigation system the week of July 9. The copper wire was worth $50, but the damages to the irrigation system totaled $10,000. A Coffee County farmer suffered a similar loss in June. He said knocking out a farmer's irrigation system in the summer could have a critical impact on his crops. Copper thefts from farms have become such a problem that Alfa Insurance is offering a reward of $10,000 for information leading to a conviction of anyone involved with copper or metal theft from irrigation equipment, chicken houses, or other equipment covered by an Alfa policy. Source: http://www.gadsdentimes.com/article/20120725/APN/1207250640

Government Sector (including Schools and Universities)

(Colorado) **Suspicious packages deemed no threat at Anchutz Medical campus.** Officials at the University of Colorado Denver Anschutz Medical campus in Aurora, Colorado, said two suspicious packages found on the campus July 23 were deemed no threat to students and faculty. "Because of the events of this past weekend, we wanted to be sure of the safety of the

campus and make sure that they were not a threat," said a spokeswoman for the university. "We brought in local authorities to look at the situation, they did just that, and they viewed it to be no threat." One of the packages was sent to a faculty member, while the other was sent to the campus' mail services. No classes were disrupted, but minor evacuations did take place, the spokeswoman said. The suspected shooter who is alleged to have killed 12 people at a nearby movie theater in Aurora was in the process of withdrawing from the school's graduate program in neurosciences. Source: http://www.denverpost.com/news/ci_21141459/suspicious-packages-deemed-no-threat-at-anchutz-medical

Agencies to dole out new hardware keys for secret networks. The Pentagon is helping civilian agencies block access to federal classified networks by anyone who does not have a new smart card, military officials announced July 19. During a closed-door U.S. House of Representatives committee hearing earlier in the day, the Secretary of Defense briefed lawmakers on the action — part of a new top-down agenda to prevent the exposure of government secrets. Defense Department officials already announced the ongoing distribution of the new tokens military employees will need to enter the Secret Internet Protocol Router Network, which handles the military's classified data. The policy announced July 19 states, "department personnel are working with other federal departments and agencies to help them issue the same cyber identity credential to all employees who need to access any of the government's secret networks." Source: http://www.nextgov.com/cybersecurity/2012/07/agencies-dole-out-new-hardware-keys-secret-networks/56907/

Information Technology and Telecommunications

1,500 severe security events detected on Black Hat WLAN. The WLAN network at Black Hat was accessed by 3,155 attendees with a maximum of 904 simultaneous clients detected and quickly contained a total of 1,561 severe independent security events. These events included more than 280 rouge access points (AP) — with some rogue APs attempting to impersonate the official event network. Other wireless attacks that were detected included Block ACK DoS attacks, Power Save DoS attacks, Deauth Broadcast, AP Spoofing, and "Hotspotter" attacks. The network also detected some malicious fragmentation-based attacks from the wired side, which were all contained very quickly. The network, which covered a 200,000 square foot facility, consisted of 23 mesh point Aruba AP-134 APs and 16 mesh portal Aruba AP-134 APs. The 16 mesh portal APs were wired into the hotel's infrastructure. Also included in the network were an Aruba 3600 Mobility Controller and an Aruba S3500 Mobility Access Switch. Source: http://www.net-security.org/secworld.php?id=13339&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

Study: Microsoft repeatedly ranks as top U.S. spammer. Microsoft has topped a list of biggest U.S. spammers for 5 out of the past 15 months, and for some of those months it ranked No. 1 in the world, according to a University of Texas (UT) study to flag the worst offenders in an effort to get them to improve their security. Based on results culled from spam block lists, researchers found that Microsoft IP addresses were responsible for a big enough volume of spam to top

their SpamRankings list for the United States in April and May 2011, and in March, April, and June 2012, said a researcher with the project at McCombs School of Business, UT Austin. The project analyzes raw data about where spam traffic comes from and tracks down what organization owns the offending IP addresses. The raw data gathered by groups outside UT, and the Microsoft rankings are based on those compiled by Passive Spam Block List. The researcher said one factor in the high volume of Microsoft spam may be that part of it is MSN, the Microsoft portal that includes its ISP. "Its purpose is to let people have access to the Internet, and that means people have their own computers, which may have all sorts of security problems," he said. Outbound spam from an organization indicates a security problem, he said, sometimes because machines have been compromised by botnets and sometimes because users have fallen for phishing ploys. Source:
http://www.networkworld.com/news/2012/072512-microsoft-spammer-261183.html?page=1

Impersonating Microsoft Exchange servers to manipulate mobile devices. At the Black Hat security conference July 26, an Australian researcher will demonstrate a proof-of-concept attack using a man-in-the-middle connection and Microsoft Exchange to conduct unauthorized remote wipes on mobile devices. According to the research presented at Black Hat, this is the beginning to further explorations of what man-in-the-middle attacks leveraging Microsoft Exchange against poorly configured mobile devices are really capable of doing. Source:
http://www.darkreading.com/vulnerability-management/167901026/security/news/240004323/

Hacker on Apple's iOS in-app purchase fix: 'Game is over'. During the week of July 9 a Russian developer hacked Apple's In-App Purchase program for all devices running iOS 3.0 or later, allowing iPhone, iPad, and iPod touch users to circumvent the payment process and essentially steal in-app content. Apple confirmed the workaround and the week of July 16 announced a temporary fix and that it would patch the holes with the release of iOS 6. July 23, the developer declared Apple's solution indeed stops his hack. In the meantime, he said the "service will still remain operational until iOS 6 comes out." Furthermore, the researcher was still working on the Mac in-app purchase hack he disclosed the week of July 16. Source:
http://www.zdnet.com/hacker-on-apples-ios-in-app-purchase-fix-game-is-over-7000001409/

Web-connected industrial controls stoke security fears. Until several days ago, anyone who researched the security of industrial control systems could have accessed the Web site of a Kansas agricultural concern and turned off all its windmills. The owner left the system connected to the open Internet without any password protections, despite warnings from Canadian manufacturer Endurance Wind Power. A cyber researcher found the vulnerability along with thousands of other exposed industrial controls, many of them in critical facilities. The research that found the lapse came from one of two new studies on the security of industrial controls that were provided to Reuters in advance of their public release at the Black Hat security conference being held the week of July 23 in Las Vegas. The research buttress concerns that critical national infrastructure in the West is more vulnerable to hacking attacks now than 2 years ago, despite its status as a top cybersecurity priority for the White House, and other parts of the federal government. Source:

http://www.reuters.com/article/2012/07/23/us-blackhat-industrialcontrols-idUSBRE86M14R20120723

Skype: Nearly half of adults don't install software updates. A new survey commissioned by Skype reveals that 40 percent of adults do not always update their software when prompted to do so, and that 25 percent skip software updates because they think they offer no real benefit. The survey was offered on Skype's behalf to 350,000 individuals in the United States, United Kingdom, and Germany by Internet pollster YouGov. A quarter of the adults surveyed said they did not understand the benefits of software updates or what they were supposed to do. About the same number said they did not know how to check for updates, and another quarter said they would need to be prompted to upgrade their software at least twice before they would do it. The respondents gave various reasons for shying away from updates. Some said they expected new versions of software would have "lots of bugs" or would crash too often, while others said they thought the updates would slow down their computers. More than a quarter of respondents said the process of updating their software just takes too long. Forty-five percent of survey participants said they did not upgrade their software because they worry about the security of their computers. Source: http://www.theregister.co.uk/2012/07/23/skype_software_update_survey/

The latest threat: A virus made just for you. The Flashback computer virus gained notoriety earlier in 2012 as the first malware to make headway against Apple's relatively untouched operating system, Mac OS X, infecting 600,000 victims' machines at the peak of the outbreak. However, computer scientists and security professionals were more worried about another aspect of the malware. The authors of Flashback used a technique that Hollywood often employs to prevent movie and music files from being copied — they added functions that bound the virus to each infected system. The use of that technique prevented security companies from running the virus in their labs. New research shows that a refinement to the technique could make automated analysis of malware nearly impossible.

Grum botnet briefly returns from the dead. The creators of the Grum botnet managed to briefly bring the spam network back from the dead before it was once again shut down. Security vendor FireEye reported the attempt to get the botnet back online took place July 23. "Over the weekend we found that the Ukrainian internet service provider (ISP) SteepHost removed the null route on three [command and control servers] that were taken down last week," a FireEye researcher said. "We immediately noticed this change and contacted SteepHost once again. After hours of negotiations, they eventually shut down these CnCs once more." Source: http://www.v3.co.uk/v3-uk/news/2193786/grum-botnet-briefly-returns-from-the-dead

Many iOS apps access personal data without user permission. One in five iOS applications can access a user's iPhone address book, two in five can track a user's location, and more than one in three store user data without encrypting it, all without explicit user permission, according to research by Bitdefender. A chief security researcher at the firm explained the company used its Clueful app, which enables iPhone owners to learn what apps may be using personal data

inappropriately, to collect data for the study. Apple removed the Clueful app from its App Store once Bitdefender collected its iOS app statistics. Source: http://www.infosecurity-magazine.com/view/27091/

National Monuments and Icons

(Arkansas; Nebraska) **Nebraska wildfires rage as dry heat scorches central U.S.** Firefighters in three Nebraska counties battled expanding wildfires July 25, and the entire town of Ola, Arkansas was evacuated because of an approaching fire, as the central part of the United States suffered through another day of stifling heat. Large fires were raging in Nebraska, where 72,400 acres had been consumed in the drought-stricken north central region of the State by July 25, authorities said. Weeks of 100-plus degree temperatures have destroyed many dryland crops across Nebraska leaving areas more susceptible to wildfires, and made conditions for firefighters nearly unbearable. A portion of the Niobrara River was declared off limits for public use and a part of Nebraska Highway 12 was closed, but reopened July 25. The Ainsworth area Chamber of Commerce pleaded for help July 25, citing the loss of grazing land for cattle and the loss of structures. Donations will be used to buy feed and hay for cattle, fencing supplies and other ranching needs, it said on its Web site. Source: http://www.propertycasualty360.com/2012/07/26/nebraska-wildfires-rage-as-dry-heat-scorches-centr?t=es-specialty

Postal and Shipping

(Missouri) **Bomb squad called after suspicious package found at post office.** A suspicious package was discovered and destroyed at a post office in Naylor, Missouri, July 24. According to the Ripley County sheriff, the postmaster discovered a small box with wires sticking out of it on the lobby counter. Deputies responded and evacuated a 300-yard perimeter. The sheriff called in the Southeast Missouri Regional Bomb Squad, which used a remote-controlled robot to enter the post office and examine the package. As the package was being removed to be X-rayed, the owner of the package arrived. “He just came up to us and said the package wasn’t dangerous,” the sheriff said. “It was a dog-shocking collar charger.” Apparently the package was accidentally left out of a larger package that was being mailed. After a few questions, the package was returned to the owner. Source: http://www.kait8.com/story/19099881/suspicious-package-found-at-naylor-post-office

Public Health

Hepatitis C probe now in 8 states. Health officials confirmed July 25 that the former medical technician at Exeter Hospital in Exeter, New Hampshire who was accused of spreading hepatitis C also worked in Pennsylvania, bringing to the total number of States where he was employed to at least eight. The announcement came as Exeter Hospital lowered the number of patients to be tested at public clinics at Exeter High School from 6,000 to 3,400. New Hampshire health officials announced July 24 they were expanding testing to those who were admitted to the ICU and who underwent inpatient surgeries between April 1, 2011, and May 25, 2012, after

learning the former employee had access to those units. The technician was accused of infecting 30 Exeter Hospital patients in its cardiac catheterization lab by shooting up the powerful painkiller Fentanyl and then returning tainted syringes to be used on other patients. Before arriving at Exeter, the technician worked in hospitals around the country as a traveling medical technician who filled temporary jobs. In addition to Pennsylvania and New Hampshire, the technician was also being investigated for work at hospitals in Arizona, Georgia, Kansas, Maryland, Michigan, and New York. Source: http://www.unionleader.com/article/20120726/NEWS12/707269913

Multistate outbreak of human Salmonella Hadar infections linked to live poultry. The Centers for Disease Control and Prevention (CDC) is collaborating with public health and agriculture officials in many States and the U.S. Department of Agriculture to investigate an outbreak of human Salmonella Hadar infections linked to chicks, ducklings, and other live poultry from Hatchery B in Idaho, a July 23 notice states. Public health investigators are using the PulseNet system to identify cases of illness that may be part of these outbreaks. As of July 19, 37 people infected with the outbreak strain of Salmonella Hadar have been reported from 11 States: Arizona (2), California (1), Colorado (3), Idaho (5), Illinois (2), Oregon (5), Tennessee (2), Texas (1), Utah (5), Washington (9), and Wyoming (2). Illnesses began between March 19 and July 6. Among 26 ill persons with available information, 8 have been hospitalized. Twenty-four of 27 ill persons interviewed reported contact with live poultry before becoming ill. Live poultry were purchased from agricultural feed stores or direct from the mail-order hatchery. Source: http://www.cdc.gov/salmonella/hadar-live-poultry-07-12/index.html

(Massachusetts) **Laptop theft may affect 3,900 Beth Israel patients.** About 3,900 Beth Israel Deaconess Medical Center patients in Boston were sent letters alerting them that some of their personal health information may have been breached after a physician's personal laptop computer was stolen from a hospital office, hospital officials said July 20. The theft occurred May 22, and the stolen laptop, which contained a tracking device, has not been recovered. Police were notified and a suspect was arrested in the case. The hospital hired a national forensic firm to investigate whether data were compromised, and it found no indication that any information had been misused. Beth Israel Deaconess routinely protects information on company-issued computers by encrypting the material with software, but in this case the stolen laptop was the physician's personal device that was used for some office work. The event prompted an immediate policy change at the hospital. "We have said to our employees that there is now a mandatory encryption program. So any device that is used in any way with our data, whether it is patient-related or administrative, it must be encrypted," said the hospital's chief information officer. "We are creating depots where employees bring in their devices and we will encrypt them on their behalf," he said. "We will ensure that it has appropriate antivirus protection and up-to-date software patches." The 6,000 employees at the hospital's Longwood-area medical campus own an estimated 1,500 personal electronic devices that might be used for work. The process of encrypting is expected to take about 3 months. Source: http://bostonglobe.com/lifestyle/health-wellness/2012/07/20/patient-information-may-have-been-breached-after-laptop-stolen-beth-israel-deaconess/JobJhtGnm7C8z0QthhG5SP/story.html

Transportation

(Ohio) **1 Ohio bridge bomb plot suspect pleads guilty.** One of five men charged with plotting to bomb an Ohio highway bridge pleaded guilty July 25 and agreed to testify against his co-defendants. The Cleveland man, who has a criminal record for theft and breaking and entering, pleaded to all three counts against him in federal court. His attorney said the defendant hopes to get leniency in return for his testimony. With the plea and offer of testimony for the prosecution, he could face 15 years to nearly 20 years in prison. Source: http://www.seattlepi.com/news/article/1-bridge-bomb-plot-suspect-in-Ohio-pleads-guilty-3734201.php

Water and Dams

Nothing Significant to Report

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168